

## 2005 DRAFTING REQUEST

### Assembly Substitute Amendment (ASA-SB164)

Received: 02/03/2006

Received By: csundber

Wanted: As time permits

Identical to LRB:

For: Jeff Fitzgerald (608) 266-2540

By/Representing: Jim Bender

This file may be shown to any legislator: NO

Drafter: csundber

May Contact:

Addl. Drafters:

Subject: Trade Regulation - electron com  
Trade Regulation - other

Extra Copies:

Submit via email: YES

Requester's email: Rep.Fitzgerald@legis.state.wi.us

Carbon copy (CC:) to:

---

#### Pre Topic:

No specific pre topic given

---

#### Topic:

Change definition of personal information, permit person who receives notice to request entity to identify the personal information that was accessed, other changes

---

#### Instructions:

See Attached

---

#### Drafting History:

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/?	csundber 02/06/2006	jdye 02/07/2006					
/1	csundber 02/07/2006	wjackson 02/07/2006	rschluet 02/07/2006		sbasford 02/07/2006	sbasford 02/07/2006	
/2			rschluet 02/07/2006		lnorthro 02/07/2006	lnorthro 02/07/2006	

FE Sent For:

<END>

## 2005 DRAFTING REQUEST

### Assembly Substitute Amendment (ASA-SB164)

Received: 02/03/2006

Received By: csundber

Wanted: As time permits

Identical to LRB:

For: Jeff Fitzgerald (608) 266-2540

By/Representing: Jim Bender

This file may be shown to any legislator: NO

Drafter: csundber

May Contact:

Addl. Drafters:

Subject: Trade Regulation - electron com  
Trade Regulation - other

Extra Copies:

Submit via email: YES

Requester's email: Rep.Fitzgerald@legis.state.wi.us

Carbon copy (CC:) to:

---

#### Pre Topic:

No specific pre topic given

---

#### Topic:

Change definition of personal information, permit person who receives notice to request entity to identify the personal information that was accessed, other changes

---

#### Instructions:

See Attached

---

#### Drafting History:

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/?	csundber 02/06/2006	jdye 02/07/2006					
/1		1/2 wj 2/7	rschluet 02/07/2006		sbasford 02/07/2006	sbasford 02/07/2006	

FE Sent For:

<END>

**2005 DRAFTING REQUEST**

**Assembly Substitute Amendment (ASA-SSA3-SB164)**

Received: 02/03/2006

Received By: **csundber**

Wanted: As time permits

Identical to LRB:

For: **Jeff Fitzgerald (608) 266-2540**

By/Representing: **Jim Bender**

This file may be shown to any legislator: **NO**

Drafter: **csundber**

May Contact:

Addl. Drafters:

Subject: **Trade Regulation - electron com**  
**Trade Regulation - other**

Extra Copies:

Submit via email: **YES**

Requester's email: **Rep.Fitzgerald@legis.state.wi.us**

Carbon copy (CC:) to:

---

**Pre Topic:**

No specific pre topic given

---

**Topic:**

Change definition of personal information, permit person who receives notice to request entity to identify the personal information that was accessed, other changes

---

**Instructions:**

See Attached

---

**Drafting History:**

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/?	csundber	1 2 7 jld	275	275			

FE Sent For:

<END>

2/3/06 Jim Bender / Jeff Fitzgerald

SA to SSA 3 to SB 164.

- ✓ 1. Add: person who receives notice may  
x request that the notifying entity identify  
The personal info. that was accessed  
without authorization.
- ✓ 2. Change 30 business days to 45  
x calendar days.
- ✓ 3. Change definition of "personal info"  
x using language from MN, except don't  
require linkage between account number  
and security code/access number (PIN).  
Add DNA and biometric data from 943.201(1)
- ✓ 4. Notification: for entities that have info  
x but don't own it (~~ie, a licensee~~); if there  
is no contract between ~~licensee and~~ owner  
of data, require that ~~licensee~~ notify owner  
of unauthorized access (in addition to person  
who is subject of the data).
- ✓ 5. ~~Change from entity that "stores" to entity~~  
x ~~that "licenses" P.I.~~
- ✓ 6. Change (2) (cm) 1. exception to "does not  
x create a material risk of identity theft or fraud  
for the person to whom the personal information  
pertains"

Kusson/Amend Amend

2005 - 2006 LEGISLATURE

**SENATE SUBSTITUTE AMENDMENT 3,  
TO 2005 SENATE BILL 164**

November 1, 2005 - Offered by Senator KANAVAS

- 1 **AN ACT to create** 895.507 of the statutes; **relating to:** notice regarding unauthorized  
2 acquisition of personal information.

---

***Analysis by the Legislative Reference Bureau***

This substitute amendment requires an entity that possesses certain personal information about an individual to notify the individual when the information is accessed by a person who the entity has not authorized to do so (unauthorized access). The substitute amendment's notice requirements apply to entities, including the state and local governments, that do any of the following: conduct business in Wisconsin and maintain personal information in the ordinary course of business; store personal information in this state; maintain a depository account for a Wisconsin resident; or lend money to a Wisconsin resident.

Under the substitute amendment, personal information includes any of the following information about an individual, if accompanied by the name of the individual to whom the information pertains: driver's license number; social security number; depository account number and certain other financial information; deoxyribonucleic acid (DNA) profile and other biometric data; and certain other information that can be used to obtain money, goods, or services, or other things of value. Personal information does not include information that is lawfully available to the public or information that is encrypted.

As to an entity whose principal place of business is located in Wisconsin or that stores personal information in Wisconsin, if the entity knows or has reason to know

1 of an unauthorized access, the substitute amendment requires the entity to make reasonable  
2 efforts to notify the individual that is the subject of the personal information (subject) that the  
3 individual's personal information has been accessed. As to an entity whose principal place  
4 of business is not located in Wisconsin, if the entity knows or has reason to know of an  
5 unauthorized access involving information pertaining to a Wisconsin resident, the substitute  
6 amendment requires the entity to make reasonable efforts to notify the subject. An entity is  
7 not required to give notice if the acquisition of personal information does not compromise the  
8 security, confidentiality, or integrity of the personal information, or if the personal  
9 information was acquired in good faith by an employee of the entity and the personal  
10 information is used for a lawful purpose of the entity.

11 Under the substitute amendment, an entity required to notify a subject must, within a  
12 reasonable time not to exceed 30 business days after learning of the unauthorized access,  
13 inform the subject that the entity knows of the unauthorized use of personal information  
14 pertaining to the subject. The entity must deliver the notice by mail or by another method the  
15 entity has previously used to communicate with the subject. If the entity cannot reasonably  
16 determine the subject's mailing address, the entity may notify the subject by another means  
17 reasonably calculated to provide actual notice to the subject. Under the substitute  
18 amendment, a law enforcement agency may request an entity to delay a required notice for  
19 any period of time in order to protect an investigation or homeland security. An entity that  
20 receives such a request must begin the notification process after the requested delay period.

21 The substitute amendment contains exemptions from the notice requirements for  
22 certain entities that are subject to, and in compliance with, certain requirements imposed by  
23 federal law and regulations that generally relate to the privacy and security of medical and  
24 financial data. The substitute amendment also prohibits the enactment or enforcement by a  
25 city, village, town, or county of an ordinance or regulation that relates to notice or disclosure  
26 of the unauthorized acquisition of personal information.

27 The substitute amendment provides that failure to comply with the substitute  
28 amendment's requirements is not negligence or a breach of a legal duty, but may be evidence  
29 of negligence or a breach of a legal duty.  
30  
31

---

32  
33 *The people of the state of Wisconsin, represented in senate and assembly, do*  
34 *enact as follows:*

35 SECTION 1. 895.507 of the statutes is created to read:

36 **895.507 Notice of unauthorized acquisition of personal information.**

37 (1) DEFINITIONS. In this section:

1 (a) 1. "Entity" means a person, other than an individual, that does any of the  
2 following:

3 a. Conducts business in this state and maintains personal information in the  
4 ordinary course of business.

5 b. Stores personal information in this state.

6 c. Maintains for a resident of this state a depository account as defined in s.  
7 815.18 (2) (e).

8 d. Lends money to a resident of this state.

9 2. "Entity" includes all of the following:

10 a. The state and any office, department, independent agency, authority,  
11 institution, association, society, or other body in state government created or  
12 authorized to be created by the constitution or any law, including the legislature and  
13 the courts.

14 b. A city, village, town, or county.

15 (am) "Name" means an individual's last name combined with the individual's  
16 first name or first initial.

17 {(b) "Personal information" means any of the information specified in s. 943.201

18 (1) (b) 4., 5., 9., 11., .<sup>1</sup> if all of the following apply:

---

<sup>1</sup> The data elements for which notice would be required differ from those in the 21 states that have enacted data security breach legislation (by adding data elements, like any account number or unique physical representation, and omitting others, like government issued id numbers). Because most security breaches involve data of individuals in more than one state, it would be very helpful if the data elements covered by this bill were consistent with those in most other state laws. (This is our second suggested (b) paragraph, after the "or").

If the sponsors do not want to conform the data elements in Wisconsin law to those in other states, we urge that they at least delete the cross-reference to paragraphs 12 a. and c. and 13 of section 943.201 because they are phrased in an overbroad way that sweeps in data elements that are not at all sensitive. An "an individual's code or account number" and "any other means of account access" if they "can be used to obtain money, goods, services or any other thing of value or benefit" see section 942.201(12)a. and c, are overbroad because they cover a simple telephone number, email or Instant Messaging address, or any other communications account number. The term used in most other state laws is "financial account number" because these pose a threat of identity theft or fraud. Another term that would work is "credit account number." Furthermore, one of the data elements in paragraph 13, "any unique physical representation", would likely cover a simple sketch or photograph of individual.



1           1. The information is accompanied by the name of the individual to whom the  
2 information pertains.


3           2. The information is not publicly available.

4           3. The information is not encrypted, redacted or otherwise protected by a method that  
5 renders the information unusable or unreadable.} OR

6           (b) "Personal information" means, notwithstanding section  
7 943.201, an individual's first name or first initial and last name, in  
8 combination with and linked to any one or more of the following  
9 data elements, when the data elements are not encrypted, redacted,  
10 or altered by any method or technology in such a manner that the  
11 data elements are unreadable:

12           (i) Social security number; <sup>5</sup>


13           (ii) Driver's license number or state identification card <sup>4</sup>  
14 number;

15           (iii) Financial account number or credit or debit card number, <sup>12</sup>  
16 in combination with and linked to any required security code, access   
17 code, or password that would permit access to an individual's  
18 financial account.}

19           (c) "Publicly available information" means any information that an entity  
20 reasonably believes is one of the following:

21           1. Lawfully made widely available through any media.

22           2. Lawfully made available to the general public from federal, state, or local  
23 government records or disclosures to the general public that are required to be made  
24 by federal, state, or local law.

25           (2) NOTICE REQUIRED. (a) If an entity  whose principal place of business is  
26 located in this state or an entity that owns or licenses <sup>2</sup> personal information of a resident of

<sup>2</sup> Every other state breach notice law requires notice by the entity that "owns or licenses" the information, rather than the entity that "stores" the information (which may be a third party service provider). This other approach is better for consumers, because the entity that owns the data is in almost all cases the entity with whom

1       <sup>3</sup>this state know that personal information in the entity's possession has been acquired by a  
 2       person whom the entity has not authorized to acquire the personal information, the entity  
 3       shall make reasonable efforts to notify each subject of the personal information. The  
 4       notice shall indicate that the entity knows of the unauthorized acquisition of  
 5       personal information pertaining to the subject of the personal information.

6               (b) Any person or business that maintains computerized data that includes personal  
 7       information that the person or business does not own shall notify the owner or licensee of the  
 8       information of any breach of the security of the data as soon as practicable following  
 9       discovery, if the personal information was, or is reasonably believed to have been, acquired  
 10      by an unauthorized person.<sup>4</sup>

11              <sup>5</sup>(c) Notwithstanding pars. (a) and (b), an entity is not required to provide  
 12      notice of the acquisition of personal information if any of the following apply:

13              1. The acquisition of personal information does not <sup>(4)</sup>create a material risk of identity  
 14      theft or fraud to the resident <sup>(of this state)</sup> to whom such information pertains or does not<sup>6</sup>  
 15      compromise the security, confidentiality, or integrity of personal information in the entity's  
 16      possession.

---

the consumer has a business relationship. When the consumer receives notice from entities with whom he or she has a relationship (as opposed to a third party service provider the consumer will not recognize), the consumer will be far more likely to open and read the notice.

<sup>3</sup> This change is necessary to avoid requiring duplicative notice to residents of other states. All the current state laws impose notification requirements based upon the state of residence of the individuals who are to receive notice, instead of the state where the breached entity is located. This would mean that SB 164 would impose a duplicative requirement under Wisconsin law, for residents of those states.

<sup>4</sup> This paragraph, found in all other state breach notice laws, requires a third party that stores information on behalf of the owner or licensee to notify the owner or licensee very quickly so that the owner or licensee can notify the affected individuals.

<sup>5</sup> This paragraph is unnecessary because paragraph (a) already requires notice by entities whose principal place of business is not located in Wisconsin.

<sup>6</sup> This change is **very important** to include so that notice is provided in situations that actually pose some material risk of identity theft or fraud to the individuals receiving notice. It is found in breach notice laws in states such as Ohio and New Jersey, as well as the ALEC model breach bill. If the change is not included, senior citizens will be needlessly scared and go to great inconvenience canceling financial accounts due to breaches that pose no risk to them, and over time consumers will receive so many notices that they will begin to ignore them and won't focus on notices concerning breaches that actually pose a risk of identity theft or fraud.

1           2. The personal information was acquired in good faith by an employee or agent  
2 of the entity, if the personal information is used for a lawful purpose of the entity.

3           (3) TIMING AND MANNER OF NOTICE. (a) Subject to sub. (5), an entity shall provide  
4 the notice required under sub. (2) to a resident of this state within a reasonable time, not to  
5 exceed 30 business days after the entity learns of the acquisition of personal information  
6 (pertaining to such resident.) <sup>(5)</sup>

7           (b) An entity shall provide the notice required under sub. (2) by mail or by a  
8 method the entity has previously employed to communicate with the subject of the  
9 personal information. If an entity cannot with reasonable diligence determine the  
10 mailing address of the subject of the personal information, or if the entity has not  
11 previously communicated with the subject of the personal information, the entity  
12 shall provide notice by a method reasonably calculated to provide actual notice to the  
13 subject of the personal information.

14           (3m) REGULATED ENTITIES EXEMPT. This section does not apply to any of the  
15 following:

16           (a) An entity that is subject to, and in compliance with, the privacy and security  
17 requirements of 15 USC 6801 to 6827, or a person that has a contractual obligation  
18 to such an entity to comply with the requirements of those sections, if the entity or person has  
19 in effect a policy concerning breaches of  
20 information security.

21           (b) An entity that is described in 45 CFR 164.104 (a), if the entity complies with  
22 the requirements of 45 CFR part 164.

23           (4) EFFECT ON CIVIL CLAIMS. Failure to comply with this section is not negligence  
24 or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.

<sup>7</sup> This is a very important technical change. It clarifies that the 30 day deadline for providing notice is tied to the specific individuals as to whom a breach is learned to have occurred. Sometimes, an entity will discover that some individuals' information was breached and then weeks or even months later, will learn that other individuals' information was also breached. In these circumstances, the entity does not even know that the second group of individuals was affected by the breach and cannot provide notice to them on the same timetable.

**(5) REQUEST BY LAW ENFORCEMENT NOT TO NOTIFY.** A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required under sub. (2) for any period of time and the notification process required under sub. (2) shall begin at the end of that time period. Notwithstanding subs. (2) and (3), if an entity receives such a request, the entity may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.

**(6m) LOCAL ORDINANCES OR REGULATIONS PROHIBITED.** No city, village, town, or county may enact or enforce an ordinance or regulation that relates to notice or disclosure of the unauthorized acquisition of personal information.

**(7m) EFFECT OF FEDERAL LEGISLATION.** If the joint committee on administrative rules determines that the federal government has enacted legislation that imposes notice requirements substantially similar to the requirements of this section and determines that the legislation does not preempt this section, the joint committee on administrative rules shall submit to the revisor of statutes for publication in the Wisconsin administrative register a notice of its determination. This section does not apply after publication of a notice under this subsection.

(END)

**ASSEMBLY SUBSTITUTE AMENDMENT 1,  
TO 2005 ASSEMBLY BILL 836**

November 30, 2005 – Offered by Representatives J. FITZGERALD, GUNDRUM, DAVIS, NISCHKE, LOEFFELHOLZ, JENSEN, BIES, HINES, OTT, BALLWEG, KLEEFISCH, OWENS, FREESE, HUNDERTMARK, MCCORMICK, CULLEN, KRAWCZYK and MONTGOMERY.

- 1    **AN ACT** *to create* 895.507 of the statutes; **relating to:** notice regarding  
2    unauthorized acquisition of personal information.

---

***Analysis by the Legislative Reference Bureau***

This substitute amendment requires an entity that possesses certain personal information about an individual to notify the individual when the information is accessed by a person who the entity has not authorized to do so (unauthorized access). The substitute amendment's notice requirements apply to entities, including the state and local governments, that do any of the following: conduct business in Wisconsin and maintain personal information in the ordinary course of business; store personal information in this state; maintain a depository account for a Wisconsin resident; or lend money to a Wisconsin resident.

Under the substitute amendment, personal information includes any of the following information about an individual, if accompanied by the name of the individual to whom the information pertains: driver's license number; social security number; depository account number and certain other financial information; deoxyribonucleic acid (DNA) profile and other biometric data; and certain other information that can be used to obtain money, goods, or services, or other things of value. Personal information does not include information that is lawfully available to the public or information that is encrypted.

As to an entity whose principal place of business is located in Wisconsin or that stores personal information in Wisconsin, if the entity knows or has reason to know

of an unauthorized access, the substitute amendment requires the entity to make reasonable efforts to notify the individual that is the subject of the personal information (subject) that the individual's personal information has been accessed. As to an entity whose principal place of business is not located in Wisconsin, if the entity knows or has reason to know of an unauthorized access involving information pertaining to a Wisconsin resident, the substitute amendment requires the entity to make reasonable efforts to notify the subject. An entity is not required to give notice if the acquisition of personal information does not compromise the security, confidentiality, or integrity of the personal information, or if the personal information was acquired in good faith by an employee of the entity and the personal information is used for a lawful purpose of the entity.

Under the substitute amendment, an entity required to notify a subject must, within a reasonable time not to exceed 30 business days after learning of the unauthorized access, inform the subject that the entity knows of the unauthorized use of personal information pertaining to the subject. The entity must deliver the notice by mail or by another method the entity has previously used to communicate with the subject. If the entity cannot reasonably determine the subject's mailing address, the entity may notify the subject by another means reasonably calculated to provide actual notice to the subject. Under the substitute amendment, a law enforcement agency may request an entity to delay a required notice for any period of time in order to protect an investigation or homeland security. An entity that receives such a request must begin the notification process after the requested delay period.

The substitute amendment contains exemptions from the notice requirements for certain entities that are subject to, and in compliance with, certain requirements imposed by federal law and regulations that generally relate to the privacy and security of medical and financial data. The substitute amendment also prohibits the enactment or enforcement by a city, village, town, or county of an ordinance or regulation that relates to notice or disclosure of the unauthorized acquisition of personal information.

The substitute amendment provides that failure to comply with the substitute amendment's requirements is not negligence or a breach of a legal duty, but may be evidence of negligence or a breach of a legal duty.

---

***The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:***

- 1        **SECTION 1.** 895.507 of the statutes is created to read:
- 2        **895.507 Notice of unauthorized acquisition of personal information.**
- 3        **(1) DEFINITIONS.** In this section:

1 (a) 1. "Entity" means a person, other than an individual, that does any of the  
2 following:

3 a. Conducts business in this state and maintains personal information in the  
4 ordinary course of business.

5 b. Stores personal information in this state.

6 c. Maintains for a resident of this state a depository account as defined in s.  
7 815.18 (2) (e).

8 d. Lends money to a resident of this state.

9 2. "Entity" includes all of the following:

10 a. The state and any office, department, independent agency, authority,  
11 institution, association, society, or other body in state government created or  
12 authorized to be created by the constitution or any law, including the legislature and  
13 the courts.

14 b. A city, village, town, or county.

15 (am) "Name" means an individual's last name combined with the individual's  
16 first name or first initial.

17 (b) "Personal information" means any of the information specified in s. 943.201

18 (1) (b) 4., 5., 9., 11., 12. a. and c., and 13. if all of the following apply:

19 1. The information is accompanied by the name of the individual to whom the  
20 information pertains.

21 2. The information is not publicly available.

22 3. The information is not encrypted.

23 (c) "Publicly available information" means any information that an entity  
24 reasonably believes is one of the following:

25 1. Lawfully made widely available through any media.

1           2. Lawfully made available to the general public from federal, state, or local  
2 government records or disclosures to the general public that are required to be made  
3 by federal, state, or local law.

4           (2) NOTICE REQUIRED. (a) If an entity whose principal place of business is  
5 located in this state or an entity that <sup>3</sup>stores personal information in this state knows  
6 that personal information in the entity's possession has been acquired by a person  
7 whom the entity has not authorized to acquire the personal information, the entity  
8 shall make reasonable efforts to notify each subject of the personal information. The  
9 notice shall indicate that the entity knows of the unauthorized acquisition of  
10 personal information pertaining to the subject of the personal information.

11           (b) If an entity whose principal place of business is not located in this state  
12 knows that personal information pertaining to a resident of this state has been  
13 acquired by a person whom the entity has not authorized to acquire the personal  
14 information, the entity shall make reasonable efforts to notify each resident of this  
15 state who is the subject of the personal information. The notice shall indicate that  
16 the entity knows of the unauthorized acquisition of personal information pertaining  
17 to the resident of this state who is the subject of the personal information.

18           (cm) Notwithstanding pars. (a) and (b), an entity is not required to provide  
19 notice of the acquisition of personal information if any of the following apply:

20           1. The acquisition of personal information does not <sup>4</sup>compromise the security,  
21 confidentiality, or integrity of personal information in the entity's possession.

22           2. The personal information was acquired in good faith by an employee or agent  
23 of the entity, if the personal information is used for a lawful purpose of the entity.

24           (3) TIMING AND MANNER OF NOTICE. (a) Subject to sub. (5), an entity shall provide  
25 the notice required under sub. (2) within a reasonable time, not to exceed (30 business)

45 ACTUAL



5

1 days after the entity learns of the acquisition of personal information. A  
2 determination as to reasonableness under this paragraph shall include  
3 consideration of the number of notices that an entity must provide and the methods  
4 of communication available to the entity.

5 (b) An entity shall provide the notice required under sub. (2) by mail or by a  
6 method the entity has previously employed to communicate with the subject of the  
7 personal information. If an entity cannot with reasonable diligence determine the  
8 mailing address of the subject of the personal information, and if the entity has not  
9 previously communicated with the subject of the personal information, the entity  
10 shall provide notice by a method reasonably calculated to provide actual notice to the  
11 subject of the personal information. 1

12 (3m) REGULATED ENTITIES EXEMPT. This section does not apply to any of the  
13 following:

14 (a) An entity that is subject to, and in compliance with, the privacy and security  
15 requirements of 15 USC 6801 to 6827, or a person that has a contractual obligation  
16 to such an entity, if the entity or person has in effect a policy concerning breaches of  
17 information security.

18 (b) An entity that is described in 45 CFR 164.104 (a), if the entity complies with  
19 the requirements of 45 CFR part 164.

20 (4) EFFECT ON CIVIL CLAIMS. Failure to comply with this section is not negligence  
21 or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.

22 (5) REQUEST BY LAW ENFORCEMENT NOT TO NOTIFY. A law enforcement agency  
23 may, in order to protect an investigation or homeland security, ask an entity not to  
24 provide a notice that is otherwise required under sub. (2) for any period of time and  
25 the notification process required under sub. (2) shall begin at the end of that time

1 period. Notwithstanding subs. (2) and (3), if an entity receives such a request, the  
2 entity may not provide notice of or publicize an unauthorized acquisition of personal  
3 information, except as authorized by the law enforcement agency that made the  
4 request.

5 **(6m)** LOCAL ORDINANCES OR REGULATIONS PROHIBITED. No city, village, town, or  
6 county may enact or enforce an ordinance or regulation that relates to notice or  
7 disclosure of the unauthorized acquisition of personal information.

8 **(7m)** EFFECT OF FEDERAL LEGISLATION. If the joint committee on administrative  
9 rules determines that the federal government has enacted legislation that imposes  
10 notice requirements substantially similar to the requirements of this section and  
11 determines that the legislation does not preempt this section, the joint committee on  
12 administrative rules shall submit to the revisor of statutes for publication in the  
13 Wisconsin administrative register a notice of its determination. This section does not  
14 apply after publication of a notice under this subsection.

15  (END)

a document evidencing a chose in action or other intangible right, value means either the market value of the chose in action or other right or the intrinsic value of the document, whichever is greater. If the thief gave consideration for, or had a legal interest in, the stolen property, the amount of such consideration or value of such interest shall be deducted from the total value of the property.

(e) "Vulnerable adult" has the meaning given in s. 940.285 (1) (e).

(3) PENALTIES. Whoever violates sub. (1):

(a) If the value of the property does not exceed \$2,500, is guilty of a Class A misdemeanor.

(bf) If the value of the property exceeds \$2,500 but does not exceed \$5,000, is guilty of a Class I felony.

(bm) If the value of the property exceeds \$5,000 but does not exceed \$10,000, is guilty of a Class H felony.

(c) If the value of the property exceeds \$10,000, is guilty of a Class G felony.

(d) If any of the following circumstances exists, is guilty of a Class H felony:

1. The property is a domestic animal.

3. The property is taken from a building which has been destroyed or left unoccupied because of physical disaster, riot, bombing or the proximity of battle.

4. The property is taken after physical disaster, riot, bombing or the proximity of battle has necessitated its removal from a building.

5. The property is a firearm.

6. The property is taken from a patient or resident of a facility or program under s. 940.295 (2) or from a vulnerable adult.

(e) If the property is taken from the person of another or from a corpse, is guilty of a Class G felony.

(4) USE OF PHOTOGRAPHS AS EVIDENCE. In any action or proceeding for a violation of sub. (1), a party may use duly identified and authenticated photographs of property which was the subject of the violation in lieu of producing the property.

**History:** 1977 c. 173, 255, 447; 1983 a. 189; 1987 a. 266; 1991 a. 39; 1993 a. 213, 445, 486; 2001 a. 16, 109.

**Cross-reference:** Misappropriation of funds by contractor or subcontractor as theft, see s. 779.02 (5).

If one person takes property from the person of another, and a 2nd person carries it away, the evidence may show a theft from the person under subs. (1) (a) and (3) (d) 2., either on a theory of conspiracy or of complicity. *Hawpetoss v. State*, 52 Wis. 2d 71, 187 N.W.2d 823 (1971).

Theft is a lesser included offense of robbery. *Moore v. State*, 55 Wis. 2d 1, 197 N.W.2d 820 (1972).

Attempted theft by false representation (signing another's name to a car purchase contract) is not an included crime of forgery (signing the owner's name to a car title to be traded in). *State v. Fuller*, 57 Wis. 2d 408, 204 N.W.2d 452 (1973).

Under sub. (1) (d), it is not necessary that the person who parts with property be induced to do so by a false and fraudulent scheme; the person must be deceived by a false representation that is part of such a scheme. *Schneider v. State*, 60 Wis. 2d 765, 211 N.W.2d 511 (1973).

In abolishing the action for breach of promise to marry, the legislature did not sanction either civil or criminal fraud by the breaching party against the property of a duped victim. Restrictions on civil actions for fraud are not applicable to related criminal actions. *Lambert v. State*, 73 Wis. 2d 590, 243 N.W.2d 524 (1976).

Sub. (1) (a) should be read in the disjunctive so as to prohibit both the taking of, and the exercise of unauthorized control over, property of another. The sale of stolen property is thus prohibited. *State v. Genova*, 77 Wis. 2d 141, 252 N.W.2d 380 (1977).

The state may not charge a defendant under sub. (1) (a) in the disjunctive by alleging that the defendant took and carried away or used or transferred. *Jackson v. State*, 92 Wis. 2d 1, 284 N.W.2d 685 (Ct. App. 1979).

Circumstantial evidence of owner nonconsent was sufficient to support a jury's verdict. *State v. Lund*, 99 Wis. 2d 152, 298 N.W.2d 533 (1980).

Section 943.20 (1) (e) does not unconstitutionally imprison one for debt. *State v. Roth*, 115 Wis. 2d 163, 339 N.W.2d 807 (Ct. App. 1983).

A person may be convicted under s. 943.20 (1) (a) for concealing property and be separately convicted for transferring that property. *State v. Tappa*, 127 Wis. 2d 155, 378 N.W.2d 883 (1985).

A violation of sub. (1) (d) does not require proof that the accused personally received property. *State v. O'Neil*, 141 Wis. 2d 535, 416 N.W.2d 77 (Ct. App. 1987).

"Obtains title to property," as used in sub. (1) (d), includes obtaining property under a lease by fraudulent misrepresentation. *State v. Meado*, 163 Wis. 2d 789, 472 N.W.2d 567 (Ct. App. 1991).

The federal tax on a fraudulently obtained airline ticket was properly included in its value for determining whether the offense was a felony under sub. (3). *State v. McNearney*, 175 Wis. 2d 485, N.W.2d (Ct. App. 1993).

The definition of "bailee" under s. 407.102 (1) is not applicable to sub. (1) (b); definitions of "bailment" and are "bailee" discussed. *State v. Kuhn*, 178 Wis. 2d 428, 504 N.W.2d 405 (Ct. App. 1993).

When the factual basis for a plea to felony theft does not establish the value of the property taken, the conviction must be set aside and replaced with a misdemeanor conviction. *State v. Harrington*, 181 Wis. 2d 985, 512 N.W.2d 261 (Ct. App. 1994).

The words "uses," "transfers," "conceals," and "retains possession" in sub. (1) (b) are not synonyms describing the crime of theft but describe separate offenses. A jury must be instructed that there must be unanimous agreement on the manner in which the statute was violated. *State v. Seymour*, 183 Wis. 2d 682, 515 N.W.2d 874 (1994).

Theft from the person includes theft of a purse from the handle of an occupied wheelchair. *State v. Hughes*, 218 Wis. 2d 538, 582 N.W.2d 49 (Ct. App. 1998), 97-0638.

When the victim had pushed her purse against a car door with her leg and the defendant's action caused her to fall back, dislodging the purse, his act of taking it constituted taking property from the victim's person under sub. (3) (d) 2. *State v. Graham*, 2000 WI App 138, 237 Wis. 2d 620, 614 N.W.2d 504, 99-1960.

Multiple convictions for the theft of an equal number of firearms arising from one incident did not violate the protection against double jeopardy. *State v. Trawitzki*, 2001 WI 77, 244 Wis. 2d 523, 628 N.W.2d 801, 99-2234.

Agency is not necessarily an element of theft by fraud when the accused obtains another person's property through an intermediary. *State v. Timblin*, 2002 WI App 304, 259 Wis. 2d 299, 657 N.W.2d 89, 02-0275.

Multiple charges and multiple punishments for separate fraudulent acts was not multiplicitous. *State v. Swinson*, 2003 WI App 45, 261 Wis. 2d 633, 660 N.W.2d 12, 02-0395.

A landlord who failed to return or account for a security deposit ordinarily could not be prosecuted under this section. 60 Atty. Gen. 1.

State court rulings that unauthorized control was sufficient to support a conviction under sub. (1) (d) were not an unlawful broadening of the offense so as to deprive the defendant of notice and the opportunity to defend. *Hawkins v. Mathews*, 495 F. Supp. 323 (1980).

## 943.201 Unauthorized use of an individual's personal identifying information or documents. (1) In this section:

(a) "Personal identification document" means any of the following:

1. A document containing personal identifying information.

2. An individual's card or plate, if it can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value or benefit, or if it can be used to initiate a transfer of funds.

3. Any other device that is unique to, assigned to, or belongs to an individual and that is intended to be used to access services, funds, or benefits of any kind to which the individual is entitled.

(b) "Personal identifying information" means any of the following information:

1. An individual's name.

2. An individual's address.

3. An individual's telephone number.

4. The unique identifying driver number assigned to the individual by the department of transportation under s. 343.17 (3) (a).

5. An individual's social security number.

6. An individual's employer or place of employment.

7. An identification number assigned to an individual by his or her employer.

8. The maiden name of an individual's mother.

9. The identifying number of a depository account, as defined in s. 815.18 (2) (e), of an individual.

10. An individual's taxpayer identification number.

11. An individual's deoxyribonucleic acid profile, as defined in s. 939.74 (2d) (a).

12. Any of the following, if it can be used, alone or in conjunction with any access device, to obtain money, goods, services, or any other thing of value or benefit, or if it can be used to initiate a transfer of funds:

a. An individual's code or account number.

b. An individual's electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier.

c. Any other means of account access.

13. An individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

an electronic document or record.

## 943.201 CRIMES—PROPERTY

14. Any other information or data that is unique to, assigned to, or belongs to an individual and that is intended to be used to access services, funds, or benefits of any kind to which the individual is entitled.

15. Any other information that can be associated with a particular individual through one or more identifiers or other information or circumstances.

(2) Whoever, for any of the following purposes, intentionally uses, attempts to use, or possesses with intent to use any personal identifying information or personal identification document of an individual, including a deceased individual, without the authorization or consent of the individual and by representing that he or she is the individual, that he or she is acting with the authorization or consent of the individual, or that the information or document belongs to him or her is guilty of a Class H felony:

(a) To obtain credit, money, goods, services, employment, or any other thing of value or benefit.

(b) To avoid civil or criminal process or penalty.

(c) To harm the reputation, property, person, or estate of the individual.

(3) It is an affirmative defense to a prosecution under this section that the defendant was authorized by law to engage in the conduct that is the subject of the prosecution. A defendant who raises this affirmative defense has the burden of proving the defense by a preponderance of the evidence.

(4) If an individual reports to a law enforcement agency for the jurisdiction which is the individual's residence that personal identifying information or a personal identifying document belonging to the individual reasonably appears to be in the possession of another in violation of this section or that another has used or has attempted to use it in violation of this section, the agency shall prepare a report on the alleged violation. If the law enforcement agency concludes that it appears not to have jurisdiction to investigate the violation, it shall inform the individual which law enforcement agency may have jurisdiction. A copy of a report prepared under this subsection shall be furnished upon request to the individual who made the request, subject to payment of any reasonable fee for the copy.

**History:** 1997 a. 101; 2001 a. 109; 2003 a. 36.

A violation of sub. (2) is a continuing offense. *State v. Ramirez*, 2001 WI App 158, 246 Wis. 2d 802, 633 N.W.2d 656, 00-2605.

Because bail is statutorily defined as "monetary conditions of release," and can be expressed as cash, a bond, or both, one who misappropriates another's identity and uses it to obtain lower bail in a criminal case has done so to obtain credit or money within the meaning of this section. *State v. Peters*, 2003 WI 88, 263 Wis. 2d 475, 665 N.W.2d 171, 01-3267.

### 943.203 Unauthorized use of an entity's identifying information or documents. (1) In this section:

(a) "Entity" means a person other than an individual.

(b) "Identification document" means any of the following:

1. A document containing identifying information.

2. An entity's card or plate, if it can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value or benefit, or if it can be used to initiate a transfer of funds.

3. Any other device that is unique to, assigned to, or belongs to an entity and that is intended to be used to access services, funds, or benefits of any kind to which the entity is entitled.

(c) "Identifying information" means any of the following information:

1. An entity's name.

2. An entity's address.

3. An entity's telephone number.

4. An entity's employer identification number.

5. The identifying number of an entity's depository account, as defined in s. 815.18 (2) (e).

6. Any of the following, if it can be used, alone or in conjunction with any access device, to obtain money, goods, services, or

any other thing of value or benefit, or if it can be used to initiate a transfer of funds:

a. An entity's code or account number.

b. An entity's electronic serial number, mobile identification number, entity identification number, or other telecommunications service, equipment, or instrument identifier.

c. Any other means of account access.

7. Any other information or data that is unique to, assigned to, or belongs to an entity and that is intended to be used to access services, funds, or benefits of any kind to which the entity is entitled.

8. Any other information that can be associated with a particular entity through one or more identifiers or other information or circumstances.

(2) Whoever, for any of the following purposes, intentionally uses, attempts to use, or possesses with intent to use any identifying information or identification document of an entity without the authorization or consent of the entity and by representing that the person is the entity or is acting with the authorization or consent of the entity is guilty of a Class H felony:

(a) To obtain credit, money, goods, services, or anything else of value or benefit.

(b) To harm the reputation or property of the entity.

(3) It is an affirmative defense to a prosecution under this section that the defendant was authorized by law to engage in the conduct that is the subject of the prosecution. A defendant who raises this affirmative defense has the burden of proving the defense by a preponderance of the evidence.

(4) If an entity reports to a law enforcement agency for the jurisdiction in which the entity is located that identifying information or an identification document belonging to the entity reasonably appears to be in the possession of another in violation of this section or that another has used or has attempted to use it in violation of this section, the agency shall prepare a report on the alleged violation. If the law enforcement agency concludes that it appears not to have jurisdiction to investigate the violation, it shall inform the entity which law enforcement agency may have jurisdiction. A copy of a report prepared under this subsection shall be furnished upon request to the entity that made the request, subject to payment of any reasonable fee for the copy.

**History:** 2003 a. 36, 320.

**943.205 Theft of trade secrets. (1)** Whoever with intent to deprive or withhold from the owner thereof the control of a trade secret, or with intent to appropriate a trade secret to his or her own use or the use of another not the owner, and without authority of the owner, does any of the following may be penalized as provided in sub. (3):

(a) Takes, uses, transfers, conceals, exhibits or retains possession of property of the owner representing a trade secret.

(b) Makes or causes to be made a copy of property of the owner representing a trade secret.

(c) Obtains title to property representing a trade secret or a copy of such property by intentionally deceiving the owner with a false representation which is known to be false, made with intent to defraud, and which does defraud the person to whom it is made. "False representation" includes a promise made with intent not to perform if it is a part of a false and fraudulent scheme.

(2) In this section:

(a) "Copy" means any facsimile, replica, photograph or other reproduction of any property and any notation, drawing or sketch made of or from any property.

(b) "Owner" includes a co-owner of the person charged and a partnership of which the person charged is a member, unless the person charged and the victim are husband and wife.

(c) "Property" includes without limitation because of enumeration any object, material, device, substance, writing, record, recording, drawing, sample, specimen, prototype, model,

KEY: ~~stricken~~ = removed, old language. underscored = added, new language.

[Authors and Status](#) ■ [List versions](#)

1.1 A bill for an act  
1.2 relating to commerce; requiring businesses that  
1.3 possess personal data to notify persons whose personal  
1.4 information has been disclosed to unauthorized  
1.5 persons; proposing coding for new law in Minnesota  
1.6 Statutes, chapter 325E.

- 2.20 elements, when either the name or the data elements is not  
2.21 encrypted:
- 2.22 (1) Social Security number;  
2.23 (2) driver's license number or Minnesota identification  
2.24 card number; or  
2.25 (3) account number or credit or debit card number, in  
2.26 combination with any required security code, access code, or  
2.27 password that would permit access to an individual's financial  
2.28 account.
- 2.29 (f) For purposes of this section, "personal information"  
2.30 does not include publicly available information that is lawfully  
2.31 made available to the general public from federal, state, or  
2.32 local government records.
- 2.33 (g) For purposes of this section, "notice" may be provided  
2.34 by one of the following methods:
- 2.35 (1) written notice to the most recent available address the  
2.36 person or business has in its records;
- 3.1 (2) electronic notice, if the notice provided is consistent  
3.2 with the provisions regarding electronic records and signatures  
3.3 in United States Code, title 15, section 7001; or
- 3.4 (3) substitute notice, if the person or business  
3.5 demonstrates that the cost of providing notice would exceed  
3.6 \$250,000, or that the affected class of subject persons to be  
3.7 notified exceeds 500,000, or the person or business does not  
3.8 have sufficient contact information. Substitute notice must  
3.9 consist of all of the following:
- 3.10 (i) e-mail notice when the person or business has an e-mail  
3.11 address for the subject persons;
- 3.12 (ii) conspicuous posting of the notice on the Web site page  
3.13 of the person or business, if the person or business maintains  
3.14 one; and
- 3.15 (iii) notification to major statewide media.
- 3.16 (h) Notwithstanding paragraph (g), a person or business  
3.17 that maintains its own notification procedures as part of an  
3.18 information security policy for the treatment of personal  
3.19 information and is otherwise consistent with the timing  
3.20 requirements of this section, shall be deemed to be in  
3.21 compliance with the notification requirements of this section if  
3.22 the person or business notifies subject persons in accordance  
3.23 with its policies in the event of a breach of security of the  
3.24 system.
- 3.25 Subd. 2. [COORDINATION WITH CONSUMER REPORTING AGENCIES.]  
3.26 If a person discovers circumstances requiring notification under  
3.27 this section of more than 500 persons at one time, the person  
3.28 shall also notify, within 48 hours, all consumer reporting  
3.29 agencies that compile and maintain files on consumers on a  
3.30 nationwide basis, as defined by United States Code, title 15,  
3.31 section 1681a, of the timing, distribution, and content of the  
3.32 notices.
- 3.33 Subd. 3. [WAIVER PROHIBITED.] Any waiver of the provisions  
3.34 of this section is contrary to public policy and is void and  
3.35 unenforceable.
- 3.36 Subd. 4. [EXEMPTION.] This section does not apply to any  
4.1 "financial institution" as defined by United States Code, title  
4.2 15, section 6809(3), and to entities subject to the federal  
4.3 privacy and security regulations adopted under the federal  
4.4 Health Insurance Portability and Accountability Act of 1996,  
4.5 Public Law 104-191.
- 4.6 Subd. 5. [SECURITY ASSESSMENTS.] Each government entity  
4.7 shall conduct a comprehensive security assessment of any

- 4.8 personal information maintained by the government entity.
- 4.9 Subd. 6. [REMEDIES AND ENFORCEMENT.] The attorney general
- 4.10 shall enforce this section under section 8.31.
- 4.11 Sec. 2. [EFFECTIVE DATE.]
- 4.12 Section 1 is effective January 1, 2006.

---

Please direct all comments concerning issues or legislation  
to your House Member or State Senator.

For Legislative Staff or for directions to the Capitol, visit the Contact Us page.

General questions or comments.



In: 2/6/06  
wanted: Wed. 2/8/06

2005 - 2006 LEGISLATURE

05/12/11  
LRBs027741  
CTS:allch  
stays

ASSEMBLY SUBSTITUTE AMENDMENT  
~~TO~~ SENATE SUBSTITUTE AMENDMENT 3,

TO 2005 SENATE BILL 164

LPS - Fix request  
sheet

(D-N)

November 1, 2005 - Offered by Senator KANAVAS.

Regen

- 1 AN ACT *to create* 895.507 of the statutes; **relating to:** notice regarding
- 2 unauthorized acquisition of personal information.

✓ acquired

**Analysis by the Legislative Reference Bureau**

This substitute amendment requires an entity that possesses certain personal information about an individual to notify the individual when the information is accessed by a person who the entity has not authorized to do so (unauthorized access). The substitute amendment's notice requirements apply to entities, including the state and local governments, that do any of the following: conduct business in Wisconsin and maintain personal information in the ordinary course of business; store personal information in this state; maintain a depository account for a Wisconsin resident; or lend money to a Wisconsin resident.

acquisition

combined with

Under the substitute amendment, personal information includes any of the following information about an individual, if accompanied by the name of the individual to whom the information pertains: driver's license number; social security number; depository account number and certain other financial information; deoxyribonucleic acid (DNA) profile and other biometric data; and certain other information that can be used to obtain money, goods, or services, or other things of value. Personal information does not include information that is lawfully available to the public or information that is encrypted.

license

✓ and

As to an entity whose principal place of business is located in Wisconsin or that stores personal information in Wisconsin, if the entity knows or has reason to know

✓ licenses

financial ✓

related



of an unauthorized access, the substitute amendment requires the entity to make reasonable efforts to notify the individual that is the subject of the personal information (subject) that the individual's personal information has been accessed. As to an entity whose principal place of business is not located in Wisconsin, if the entity knows or has reason to know of an unauthorized access involving information pertaining to a Wisconsin resident, the substitute amendment requires the entity to make reasonable efforts to notify the subject. An entity is not required to give notice if the acquisition of personal information does not compromise the security, confidentiality, or integrity of the personal information, or if the personal information was acquired in good faith by an employee of the entity and the personal information is used for a lawful purpose of the entity.

Under the substitute amendment, an entity required to notify a subject must, within a reasonable time not to exceed 30 business days after learning of the unauthorized access, inform the subject that the entity knows of the unauthorized use of personal information pertaining to the subject. The entity must deliver the notice by mail or by another method the entity has previously used to communicate with the subject. If the entity cannot reasonably determine the subject's mailing address, the entity may notify the subject by another means reasonably calculated to provide actual notice to the subject. Under the substitute amendment, a law enforcement agency may request an entity to delay a required notice for any period of time in order to protect an investigation or homeland security. An entity that receives such a request must begin the notification process after the requested delay period.

The substitute amendment contains exemptions from the notice requirements for certain entities that are subject to, and in compliance with, certain requirements imposed by federal law and regulations that generally relate to the privacy and security of medical and financial data. The substitute amendment also prohibits the enactment or enforcement by a city, village, town, or county of an ordinance or regulation that relates to notice or disclosure of the unauthorized acquisition of personal information.

The substitute amendment provides that failure to comply with the substitute amendment's requirements is not negligence or a breach of a legal duty, but may be evidence of negligence or a breach of a legal duty.

*The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:*

- 1            **SECTION 1.** 895.507 of the statutes is created to read:
- 2            **895.507 Notice of unauthorized acquisition of personal information.**
- 3            **(1) DEFINITIONS.** In this section:

1 (a) 1. "Entity" means a person, other than an individual, that does any of the  
2 following:

3 a. Conducts business in this state and maintains personal information in the  
4 ordinary course of business.

5 (b) <sup>2</sup>Stores <sup>Licenses</sup> personal information in this state.

6 c. Maintains for a resident of this state a depository account as defined in s.  
7 815.18 (2) (e).

8 d. Lends money to a resident of this state.

9 2. "Entity" includes all of the following:

10 a. The state and any office, department, independent agency, authority,  
11 institution, association, society, or other body in state government created or  
12 authorized to be created by the constitution or any law, including the legislature and  
13 the courts.

14 b. A city, village, town, or county.

15 (am) "Name" means an individual's last name combined with the individual's  
16 first name or first initial.

17 (b) "Personal information" means any of the information specified in s. 943.201

18 (1) (b) 4., 5., 9., 11., 12. a. and c., and 13. if all of the following apply:

19 1. The information is accompanied by the name of the individual to whom the  
20 information pertains.

21 2. The information is not publicly available.

22 3. The information is not encrypted.

23 (c) "Publicly available information" means any information that an entity  
24 reasonably believes is one of the following:

25 1. Lawfully made widely available through any media.

2. Lawfully made available to the general public from federal, state, or local government records or disclosures to the general public that are required to be made by federal, state, or local law.

(2) NOTICE REQUIRED. (a) If an entity whose principal place of business is located in this state or an entity that ~~stores~~ <sup>maintains or licenses</sup> personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.

(b) If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident of this state who is the subject of the personal information.

(cm) Notwithstanding pars. (a) <sup>and (b)</sup> <sup>and (bm)</sup>, an entity is not required to provide notice of the acquisition of personal information if any of the following <sup>applies</sup> apply:

1. The acquisition of personal information ~~does not~~ compromise the security, confidentiality, or integrity of personal information in the entity's possession. <sup>CS</sup>

2. The personal information was acquired in good faith by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity.

(3) TIMING AND MANNER OF NOTICE. (a) Subject to sub. (5), an entity shall provide the notice required under sub. (2) within a reasonable time, not to exceed 30 business <sup>days</sup> <sup>45</sup> <sup>✓</sup>

<sup>DO</sup> create a material risk of identity theft or fraud to the subject of the personal information

1 days after the entity learns of the acquisition of personal information. A  
2 determination as to reasonableness under this paragraph shall include  
3 consideration of the number of notices that an entity must provide and the methods  
4 of communication available to the entity.

5 (b) An entity shall provide the notice required under sub. (2) by mail or by a  
6 method the entity has previously employed to communicate with the subject of the  
7 personal information. If an entity cannot with reasonable diligence determine the  
8 mailing address of the subject of the personal information, and if the entity has not  
9 previously communicated with the subject of the personal information, the entity  
10 shall provide notice by a method reasonably calculated to provide actual notice to the  
11 subject of the personal information.

12 **(3m)** REGULATED ENTITIES EXEMPT. This section does not apply to any of the  
13 following:

14 (a) An entity that is subject to, and in compliance with, the privacy and security  
15 requirements of 15 USC 6801 to 6827, or a person that has a contractual obligation  
16 to such an entity, if the entity or person has in effect a policy concerning breaches of  
17 information security.

18 (b) An entity that is described in 45 CFR 164.104 (a), if the entity complies with  
19 the requirements of 45 CFR part 164.

20 **(4)** EFFECT ON CIVIL CLAIMS. Failure to comply with this section is not negligence  
21 or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.

22 **(5)** REQUEST BY LAW ENFORCEMENT NOT TO NOTIFY. A law enforcement agency  
23 may, in order to protect an investigation or homeland security, ask an entity not to  
24 provide a notice that is otherwise required under sub. (2) for any period of time and  
25 the notification process required under sub. (2) shall begin at the end of that time

INS  
5-11

1 period. Notwithstanding subs. (2) and (3), if an entity receives such a request, the  
2 entity may not provide notice of or publicize an unauthorized acquisition of personal  
3 information, except as authorized by the law enforcement agency that made the  
4 request.

5 **(6m)** LOCAL ORDINANCES OR REGULATIONS PROHIBITED. No city, village, town, or  
6 county may enact or enforce an ordinance or regulation that relates to notice or  
7 disclosure of the unauthorized acquisition of personal information.

8 **(7m)** EFFECT OF FEDERAL LEGISLATION. If the joint committee on administrative  
9 rules determines that the federal government has enacted legislation that imposes  
10 notice requirements substantially similar to the requirements of this section and  
11 determines that the legislation does not preempt this section, the joint committee on  
12 administrative rules shall submit to the revisor of statutes for publication in the  
13 Wisconsin administrative register a notice of its determination. This section does not  
14 apply after publication of a notice under this subsection.

15 **(END)**

2005-2006 DRAFTING INSERT  
FROM THE  
LEGISLATIVE REFERENCE BUREAU

LRBs0512/1ins  
CTS:.....

LPS - inserts out of  
order

1           **Insert A-1:**

2/0 ~~2/0~~ Upon request by a person who receives a notice, an entity must identify the personal information that was acquired. ✓

Under the substitute amendment, a separate notification requirement applies to a person, other than an individual, that stores personal information pertaining to a resident of this state, but does not own or license the personal information. The requirement only applies if there is no contract between the person that stores the personal information and the person that owns or licenses the personal information. If such a person knows that personal information in the person's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity must notify the person that owns or licenses the personal information as soon as practicable.

2           **Insert 5-11:**

3           (c) Upon written request by a person who has received a notice under sub. (2), ✓  
4           the entity that provided the notice shall identify the personal information that was  
5           acquired. ✓

6           **Insert 3-17:**

7 ~~2/0~~ ~~2/0~~ an individual's last name and the individual's first name or first initial, in  
8           combination with and linked to any of the following elements, if the element is not  
9           publicly available information and is not encrypted, redacted, or altered in a manner  
10          that renders the element unreadable:

- 11           1. The individual's ~~S~~ocial ~~S~~ecurity number.  
12           2. The individual's driver's license number or state identification number.  
13           3. The number of the individual's financial account number, including a credit  
14           or debit card account number, or any security code, access code, or password that  
15           would permit access to the individual's financial account.  
16           4. The individual's ~~deoxyribonucleic acid~~ <sup>✓</sup> profile, as defined in s. 939.74 (2d) (a). ✓

1           5. The individual's unique biometric data, including fingerprint, voice print,  
2 retina or iris image, or any other unique physical representation.

3           **Insert 4-17:**

4           (bm) If a person, other than an individual,<sup>✓</sup> that stores personal information  
5 pertaining to a resident of this state, but does not own or license the personal  
6 information, knows that the personal information has been acquired by a person  
7 whom the person storing the personal information has not authorized to acquire the  
8 personal information, and the person storing the personal information has not  
9 entered into a contract with the person that owns or licenses the personal  
10 information, the person storing the personal information shall notify the person that  
11 owns or licenses the personal information of the acquisition as soon as practicable.

**DRAFTER'S NOTE**  
**FROM THE**  
**LEGISLATIVE REFERENCE BUREAU**

LRBs0512/1dn

CTS: A:...

*JLd*

Representative Fitzgerald:

This substitute amendment<sup>✓</sup> is based on instructions provided by your aide, Jim Bender. Please review it carefully to ensure it is consistent with your intent and note the following:

1. This substitute amendment alters the definition of "personal information." I have assumed that you intended to retain the exclusion for publicly available information. Is this correct?
2. The drafting instructions distinguish between entities that own or license personal information and third parties that merely store personal information that is owned by another person. The distinction is significant because of the different disclosure obligations that apply under the substitute amendment. What does it mean to "license" personal information versus merely store personal information?

Christopher T. Sundberg  
Legislative Attorney  
Phone: (608) 266-9739  
E-mail: christopher.sundberg@legis.state.wi.us



**DRAFTER'S NOTE**  
**FROM THE**  
**LEGISLATIVE REFERENCE BUREAU**

LRBs0512/1dn  
CTS:jld:rs

February 7, 2006

Representative Fitzgerald:

This substitute amendment is based on instructions provided by your aide, Jim Bender. Please review it carefully to ensure it is consistent with your intent and note the following:

1. This substitute amendment alters the definition of "personal information." I have assumed that you intended to retain the exclusion for publicly available information. Is this correct?
2. The drafting instructions distinguish between entities that own or license personal information and third parties that merely store personal information that is owned by another person. The distinction is significant because of the different disclosure obligations that apply under the substitute amendment. What does it mean to "license" personal information versus merely store personal information?

Christopher T. Sundberg  
Legislative Attorney  
Phone: (608) 266-9739  
E-mail: christopher.sundberg@legis.state.wi.us



State of Wisconsin  
2005 - 2006 LEGISLATURE

LRBs0512/14

CTS:all:rs

↑  
stays

2  
RUNR

ASSEMBLY SUBSTITUTE AMENDMENT ,  
TO 2005 SENATE BILL 164

- 1 AN ACT <sup>Regun</sup> ~~to create~~ 895.507 of the statutes; **relating to:** notice regarding
- 2 unauthorized acquisition of personal information.

---

***Analysis by the Legislative Reference Bureau***

This substitute amendment requires an entity that possesses certain personal information about an individual to notify the individual when the information is acquired by a person who the entity has not authorized to do so (unauthorized acquisition). The substitute amendment's notice requirements apply to entities, including the state and local governments, that do any of the following: conduct business in Wisconsin and maintain personal information in the ordinary course of business; license personal information in this state; maintain a depository account for a Wisconsin resident; or lend money to a Wisconsin resident.

Under the substitute amendment, personal information includes any of the following information about an individual, if combined with the name of the individual to whom the information pertains: driver's license number; social security number; financial account number and certain related information; and deoxyribonucleic acid (DNA) profile and other biometric data. Personal information does not include information that is lawfully available to the public or information that is encrypted.

As to an entity whose principal place of business is located in Wisconsin or that licenses personal information in Wisconsin, if the entity knows or has reason to know of an unauthorized acquisition, the substitute amendment requires the entity to

make reasonable efforts to notify the individual that is the subject of the personal information (subject) that the individual's personal information has been acquired. As to an entity whose principal place of business is not located in Wisconsin, if the entity knows or has reason to know of an unauthorized acquisition involving information pertaining to a Wisconsin resident, the substitute amendment requires the entity to make reasonable efforts to notify the subject. An entity is not required to give notice if the acquisition of personal information does not create a material risk of identity theft or fraud, or if the personal information was acquired in good faith by an employee of the entity and the personal information is used for a lawful purpose of the entity.

→ Under the substitute amendment, an entity required to notify a subject must, within a reasonable time not to exceed 45 ~~business~~ days after learning of the unauthorized acquisition, inform the subject that the entity knows of the unauthorized use of personal information pertaining to the subject. The entity must deliver the notice by mail or by another method the entity has previously used to communicate with the subject. If the entity cannot reasonably determine the subject's mailing address, the entity may notify the subject by another means reasonably calculated to provide actual notice to the subject. Upon request by a person who receives a notice, an entity must identify the personal information that was acquired.

Under the substitute amendment, a separate notification requirement applies to a person, other than an individual, that stores personal information pertaining to a resident of this state, but does not own or license the personal information. The requirement only applies if there is no contract between the person that stores the personal information and the person that owns or licenses the personal information. If such a person knows that personal information in the person's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity must notify the person that owns or licenses the personal information as soon as practicable.

Under the substitute amendment, a law enforcement agency may request an entity to delay a required notice for any period of time in order to protect an investigation or homeland security. An entity that receives such a request must begin the notification process after the requested delay period.

The substitute amendment contains exemptions from the notice requirements for certain entities that are subject to, and in compliance with, certain requirements imposed by federal law and regulations that generally relate to the privacy and security of medical and financial data. The substitute amendment also prohibits the enactment or enforcement by a city, village, town, or county of an ordinance or regulation that relates to notice or disclosure of the unauthorized acquisition of personal information.

The substitute amendment provides that failure to comply with the substitute amendment's requirements is not negligence or a breach of a legal duty, but may be evidence of negligence or a breach of a legal duty.

---

*The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:*

1       **SECTION 1.** 895.507 of the statutes is created to read:

2       **895.507 Notice of unauthorized acquisition of personal information.**

3       **(1) DEFINITIONS.** In this section:

4           (a) 1. "Entity" means a person, other than an individual, that does any of the  
5 following:

6           a. Conducts business in this state and maintains personal information in the  
7 ordinary course of business.

8           b. Licenses personal information in this state.

9           c. Maintains for a resident of this state a depository account as defined in s.  
10 815.18 (2) (e).

11          d. Lends money to a resident of this state.

12          2. "Entity" includes all of the following:

13           a. The state and any office, department, independent agency, authority,  
14 institution, association, society, or other body in state government created or  
15 authorized to be created by the constitution or any law, including the legislature and  
16 the courts.

17           b. A city, village, town, or county.

18           (am) "Name" means an individual's last name combined with the individual's  
19 first name or first initial.

1 (b) “Personal information” means an individual’s last name and the  
2 individual’s first name or first initial, in combination with and linked to any of the  
3 following elements, if the element is not publicly available information and is not  
4 encrypted, redacted, or altered in a manner that renders the element unreadable:

5 1. The individual’s social security number.

6 2. The individual’s driver’s license number or state identification number.

7 3. The number of the individual’s financial account number, including a credit  
8 or debit card account number, or any security code, access code, or password that  
9 would permit access to the individual’s financial account.

10 4. The individual’s deoxyribonucleic acid profile, as defined in s. 939.74 (2d) (a).

11 5. The individual’s unique biometric data, including fingerprint, voice print,  
12 retina or iris image, or any other unique physical representation.

13 (c) “Publicly available information” means any information that an entity  
14 reasonably believes is one of the following:

15 1. Lawfully made widely available through any media.

16 2. Lawfully made available to the general public from federal, state, or local  
17 government records or disclosures to the general public that are required to be made  
18 by federal, state, or local law.

19 (2) NOTICE REQUIRED. (a) If an entity whose principal place of business is  
20 located in this state or an entity that maintains or licenses personal information in  
21 this state knows that personal information in the entity’s possession has been  
22 acquired by a person whom the entity has not authorized to acquire the personal  
23 information, the entity shall make reasonable efforts to notify each subject of the  
24 personal information. The notice shall indicate that the entity knows of the

1 unauthorized acquisition of personal information pertaining to the subject of the  
2 personal information.

3 (b) If an entity whose principal place of business is not located in this state  
4 knows that personal information pertaining to a resident of this state has been  
5 acquired by a person whom the entity has not authorized to acquire the personal  
6 information, the entity shall make reasonable efforts to notify each resident of this  
7 state who is the subject of the personal information. The notice shall indicate that  
8 the entity knows of the unauthorized acquisition of personal information pertaining  
9 to the resident of this state who is the subject of the personal information.

10 (bm) If a person, other than an individual, that stores personal information  
11 pertaining to a resident of this state, but does not own or license the personal  
12 information, knows that the personal information has been acquired by a person  
13 whom the person storing the personal information has not authorized to acquire the  
14 personal information, and the person storing the personal information has not  
15 entered into a contract with the person that owns or licenses the personal  
16 information, the person storing the personal information shall notify the person that  
17 owns or licenses the personal information of the acquisition as soon as practicable.

18 (cm) Notwithstanding pars. (a), (b), and (bm), an entity is not required to  
19 provide notice of the acquisition of personal information if any of the following  
20 applies:

21 1. The acquisition of personal information does not create a material risk of  
22 identity theft or fraud to the subject of the personal information.

23 2. The personal information was acquired in good faith by an employee or agent  
24 of the entity, if the personal information is used for a lawful purpose of the entity.

1           **(3) TIMING AND MANNER OF NOTICE; OTHER REQUIREMENTS.** (a) Subject to sub. (5),  
2           an entity shall provide the notice required under sub. (2) within a reasonable time,  
3           not to exceed 45 days after the entity learns of the acquisition of personal  
4           information. A determination as to reasonableness under this paragraph shall  
5           include consideration of the number of notices that an entity must provide and the  
6           methods of communication available to the entity.

7           (b) An entity shall provide the notice required under sub. (2) by mail or by a  
8           method the entity has previously employed to communicate with the subject of the  
9           personal information. If an entity cannot with reasonable diligence determine the  
10          mailing address of the subject of the personal information, and if the entity has not  
11          previously communicated with the subject of the personal information, the entity  
12          shall provide notice by a method reasonably calculated to provide actual notice to the  
13          subject of the personal information.

14          (c) Upon written request by a person who has received a notice under sub. (2),  
15          the entity that provided the notice shall identify the personal information that was  
16          acquired.

17          **(3m) REGULATED ENTITIES EXEMPT.** This section does not apply to any of the  
18          following:

19               (a) An entity that is subject to, and in compliance with, the privacy and security  
20               requirements of 15 USC 6801 to 6827, or a person that has a contractual obligation  
21               to such an entity, if the entity or person has in effect a policy concerning breaches of  
22               information security.

23               (b) An entity that is described in 45 CFR 164.104 (a), if the entity complies with  
24               the requirements of 45 CFR part 164.

(4) **EFFECT ON CIVIL CLAIMS.** Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.

(5) REQUEST BY LAW ENFORCEMENT NOT TO NOTIFY. A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required under sub. (2) for any period of time and the notification process required under sub. (2) shall begin at the end of that time period. Notwithstanding subs. (2) and (3), if an entity receives such a request, the entity may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.

**(6m) LOCAL ORDINANCES OR REGULATIONS PROHIBITED.** No city, village, town, or county may enact or enforce an ordinance or regulation that relates to notice or disclosure of the unauthorized acquisition of personal information.

**(7m) EFFECT OF FEDERAL LEGISLATION.** If the joint committee on administrative rules determines that the federal government has enacted legislation that imposes notice requirements substantially similar to the requirements of this section and determines that the legislation does not preempt this section, the joint committee on administrative rules shall submit to the revisor of statutes for publication in the Wisconsin administrative register a notice of its determination. This section does not apply after publication of a notice under this subsection.

**(END)**